PHYSICAL TRANSPORTATION OF PHI

HIPAA Privacy ♦ April 2007

TMA Privacy Office Guidance

Records Management ♦ FOIA ♦ DUAs ♦ HIPAA Compliance ♦ Personnel Security ♦ Privacy Act/System of Records ♦ PIAs

Purpose

The purpose of this paper is to outline procedures for providing secured transportation of Protected Health Information (PHI). This guidance serves to ensure that the Military Health System (MHS) personnel apply reasonable and appropriate safeguards, as set forth by the DoD Health Information Privacy Regulation (DoD 6025.18-R) and the Health Insurance Portability and Accountability Act (HIPAA) of 1996. Additionally, it serves to ensure that reasonable efforts are made to prevent the misuse or unauthorized disclosure of PHI.

Background

HIPAA requires that covered entities implement administrative, physical and technical safeguards to ensure the proper use and protection of PHI. While HIPAA does not outline specific procedures, it is expected that covered entities will implement policies that provide reasonable guidelines for instances where PHI may be transported. These policies should delineate the circumstances under which PHI may be physically removed and how it may be removed from a designated facility to minimize the risk of that information being inadvertently lost or disclosed. Examples of these circumstances can include: medical records that are mailed to the beneficiaries at their request, beneficiaries who physically take (or bring in) reports or portions of their medical records outside of the facility to other physicians involved in their care, records that are mailed to other physicians at either the request of the beneficiary or physician directly involved in their care, records that are moved in the event a beneficiary transfers or retires. For the purposes of this paper, transportation is defined as the act of physically moving, by means of an individual, mail or courier, data from the secured, physical perimeter of one facility to another.

Guidance

<u>Paper records</u>

There are specific precautions that should be taken when transporting PHI data in a hardcopy file. The file should be wrapped or sealed in an envelope or pouch in such a manner that the PHI cannot be identified during the transportation process. The outside of the container should contain clear information regarding the addressee, which includes the name, address and telephone number where he/she can be reached. Covered entities should ensure that transported PHI be delivered only to the appropriate individuals who are authorized to receive the information. This can be accomplished by implementing a tracking method by which the sender and the recipient can sign and verify delivery and receipt of the information.

PHYSICAL TRANSPORTATION OF PHI

HIPAA Privacy ♦ April 2007

TMA Privacy Office Guidance

Records Management ♦ FOIA ♦ DUAs ♦ HIPAA Compliance ♦ Personnel Security ♦ Privacy Act/System of Records ♦ PIAs

Electronic

For those facilities with full encryption capabilities, transported CDs and other electronic media containing PHI should be encrypted. This requires the recipient of the CD to have corresponding decryption capabilities. If compatible encryption is not available to both parties, CDs/media containing PHI should be password protected. The password should be given to the recipient through a different medium, such as a separate e-mail or a phone call, never in notes or documents accompanying the actual CDs/media. The CD should be secured in such a manner that the PHI cannot be identified during the transportation process. The recipient's name, correct address and telephone number should be clearly labeled on the package. While password protection is an adequate means for safeguarding transported PHI on CDs/media, it is a less desirable method and should only be used if encryption is not available.

If transporting PHI via courier, the information must be under the courier's control at all times. A courier can be a government employee, military member or contractor who works in or supports the government office transporting the information. All data files must be in locked, carry-on luggage. While the data file may be stored in overhead or under-seat storage, it cannot be part of checked luggage when traveling. If transported by a courier, as outlined in this paragraph, the data should be encrypted.

All personnel should ensure that there is a tracking process in place for the transportation of PHI, whether in paper records or CDs/media devices, and that accountability be strongly emphasized with the establishment of this process. Existing tracking processes such as those associated with FedEx, UPS and the U.S. Postal Service are permitted, however when sending information on CDs/ media devices via these methods or by similar means, the information must be encrypted.